Amendments to the Claims

This listing of claims replaces all prior versions and listings of claims in the application:

Claims:

1. (Previously presented) Computing apparatus comprising, mounted on an assembly, main processing means, main memory means and a trusted device, each being connected for communication with one or more other components on the assembly,

the trusted device being arranged to acquire a true value of an integrity metric of the computing apparatus.

2. (Original) Computing apparatus according to claim 1, wherein the trusted device comprises device memory means and means for instructing the main processing means to determine the integrity metric and return the integrity metric for storage in the device memory means.

3. (Original) Computing apparatus according to claim 2, wherein the means for instructing the main processing means comprises, stored in the device memory means, program code native to the main processing means, and the trusted device is arranged to transfer the instructions of the program code to the main processing means.

4. (Previously presented) Computing apparatus according to claim 3, wherein the computing apparatus is arranged to cause the instructions to be the first instructions executed after release from reset.

5. (Previously presented) Computing apparatus according to claim 3, wherein the trusted device is arranged to transfer the instructions to the main processing means in response to memory read signals from the main processing means.

6. (Previously presented) Computing apparatus according to claim 1, wherein the trusted device comprises device memory means and is arranged to monitor a data bus means by which components mounted on the assembly are adapted to communicate and store in the device memory means a flag in the event the first memory read signals generated by the main processing means after the computing apparatus is released from reset are addressed to the trusted device.

7. (Previously presented) Computing apparatus according to claim 1, wherein the trusted device has stored in device memory means at least one of:

a unique identity of the trusted device;

an authenticated integrity metric generated by a trusted party; and

a secret.

8. (Original) Computing apparatus according to claim 7, wherein the trusted device has stored in device memory means a secret comprising a private asymmetric encryption key.

9. (Original) Computing apparatus according to claim 8, wherein the trusted device also has stored in device memory means a respective public encryption key that has been signed by a trusted party.

10. (Previously presented) Computing apparatus according to claim 8, wherein the trusted device has stored in device memory means an authenticated integrity metric generated by a trusted party and includes a encryption function, the trusted device being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

Claim 11. Cancelled.

12. (Previously presented) A method of operating a system comprising a trusted computing apparatus and a user, the trusted computing apparatus incorporating a trusted

device being arranged to acquire the true value of an integrity metric of the trusted computing apparatus, the method comprising the steps of:

the trusted device acquiring the true value of the integrity metric of the trusted computing apparatus;

the user generating a challenge for the trusted computing apparatus to prove its integrity and submitting the challenge to the trusted computing apparatus;

the trusted computing apparatus receiving the challenge, and the trusted device generating a response including the integrity metric and returning the response to the user; and

the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated metric for the trusted computing apparatus that had been generated by a trusted party.

13. (Original) A method according to claim 12, wherein the challenge includes a nonce, the response includes the integrity metric and the nonce, both digitally signed by the trusted device using a information security algorithm, and the user verifies the integrity metric and the nonce using a respective information security algorithm.

14. (Original) A method according to claim 13, wherein the trusted device uses a private encryption key to sign the integrity metric and the nonce, and the user uses the respective public encryption key to verify the integrity metric and the nonce.

15. (Original) A method according to claim 14, wherein the response includes a certificate held by the trusted device, which certificate has been digitally signed by a trusted party using a private encryption key of the trusted party, the certificate including the public encryption key of the trusted device, and the user verifies the certificate using the public encryption key of the trusted party and uses the public encryption key from the certificate to verify the integrity metric and the nonce.

16. (Previously presented) A method of establishing a communications channel in a system between trusted computing apparatus and remote computing apparatus, the

method including the step of the remote computing apparatus verifying the integrity of the trusted computing apparatus using the method according to claim 12, and maintaining the communications channel for further transactions in the event the integrity of the trusted computing apparatus is successfully verified by the remote computing apparatus.

17. (Previously presented) A method of verifying that trusted computing apparatus is trustworthy for use by a user for processing a particular application, the method including the step of the user verifying the integrity of the trusted computing apparatus using the method according to claim 12, and the user using the trusted computing apparatus to process the particular application in the event the integrity of the trusted computing apparatus is successfully verified by the remote computing apparatus.

Claims 18 - 21. Cancelled.

22. (Previously presented) Computing apparatus comprising an assembly; a main processor, a main memory and a trusted device, each being mounted on the assembly and connected for communication with other components mounted on the assembly, wherein the trusted device is adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric.

23. (Previously presented) Computing apparatus as claimed in claim 22, wherein the integrity metric is a digest of all or part of the basic input/output software for the computing apparatus.

24. (Previously presented) Computing apparatus as claimed in claim 22, wherein the integrity metric is a digest of all or part of the basic input/output software for components or apparatus attached to the computing apparatus.

25. (Previously presented) Computing apparatus as claimed in claim 22, wherein the trusted device is adapted to acquire a plurality of integrity metrics.

26. (Previously presented) Computing apparatus as claimed in claim 22, wherein the trusted device is adapted to be tamper resistant.

27. (Previously presented) Computing apparatus as claimed in claim 22, wherein the trusted device comprises a device memory.

28. (Previously presented) Computing apparatus as claimed in claim 27, wherein the trusted device comprises a trusted device processor.

29. (Previously presented) Computing device as claimed in claim 28, wherein the trusted device processor is adapted to instruct the main processor to determine the integrity metric and return the integrity metric for storage in the device memory.

30. (Previously presented) Computing apparatus as claimed in claim 28, wherein the trusted device processor is adapted to obtain information necessary to calculate the integrity metric and to calculate the integrity metric for storage in the device memory.

31. (Previously presented) Computing apparatus as claimed in claim 28, wherein the trusted device has a secret stored in the device memory.

32. (Previously presented) Computing apparatus as claimed in claim 31, wherein the secret comprises a private asymmetric encryption key.

33. (Previously presented) Computing apparatus as claimed in claim 32, wherein the trusted device also has stored in the device memory in the device memory a respective public encryption key that has been signed by a trusted third party.

34. (Previously presented) Computing apparatus as claimed in claim 33, wherein the trusted device also has stored in the device memory an authenticated integrity metric generated by a trusted third party and wherein the trusted device is adapted to employ an

encryption function, the trusted device processor being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

35. (Previously presented) In a computing apparatus comprising an assembly, a plurality of functional components including a main memory and a main processor mounted on the assembly, each functional component being connected for communication with one or more other functional components on the assembly, a trusted device being one of said functional components and adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric.

36. (Previously presented) A trusted device for use as a functional component in a computing apparatus, the trusted device being adapted for mounting on an assembly of the computing apparatus and being adapted for communication with other functional components of the computing apparatus, the trusted device being adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric.

37. (Previously presented) Computing apparatus as claimed in claim 36, wherein the trusted device is adapted to be tamper resistant.

38. (Previously presented) Computing apparatus as claimed in claim 36, wherein the trusted device comprises a device memory.

39. (Previously presented) Computing apparatus as claimed in claim 38, wherein the trusted device comprises a trusted device processor.

40. (Previously presented) Computing apparatus as claimed in claim 39, wherein the trusted device has a secret stored in the device memory.

41. (Previously presented) Computing apparatus as claimed in claim 40, wherein the secret comprises a private asymmetric encryption key.

42. (Previously presented) Computing apparatus as claimed in claim 41, wherein the trusted device also has stored in the device memory in the device memory a respective public encryption key that has been signed by a trusted third party.

43. (Previously presented) Computing apparatus as claimed in claim 42, wherein the trusted device also has stored in the device memory an authenticated integrity metric generated by a trusted third party and wherein the trusted device is adapted to employ an encryption function, the trusted device processor being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

44. (Previously presented) Computing apparatus as claimed in claim 1, wherein the trusted device includes non-volatile memory for storing instructions instructing the main processing means to determine the integrity metric and return the integrity metric for storage in the device memory means.

45. (Previously presented) Computing apparatus as claimed in claim 1, wherein the integrity metric is a digest of all or part of the basic input/output software for the computing apparatus.

46. (Previously presented) Computing apparatus as claimed in claim 1, wherein the integrity metric is a digest of all or part of the basic input/output software for components or apparatus attached to the computing apparatus.

47. (Previously presented) Computing apparatus as claimed in claim 1, wherein the trusted device is implemented as an application specific integrated circuit device.

48. (Previously presented) Computing apparatus as claimed in claim 1, wherein the trusted device is implemented as a programmed micro-controller.

49. (Previously presented) Computing apparatus as claimed in claim 1, wherein the trusted device is accessed by said main processing means prior to said main processing means accessing basic input/output software instructions stored in non-volatile memory during a boot process of said computing apparatus.

50. (Previously presented) A method according to claim 12, wherein the trusted device acquires the true value of the integrity metric of the trusted computing apparatus before a boot up process of the trusted computing apparatus is completed.

51. (Previously presented) The combination of claim 35 wherein the trusted device is adapted to acquire the value of the integrity metric before the computing apparatus has completed a boot up process.

52. (Currently amended) The combination of claim [[52]] 35 further including means for testing to assure that the trusted device is accessed by said main processor before said main processor accesses basic input/output instructions for booting the computing apparatus.

53. (New) Computing apparatus as claimed in claim 1 wherein said trusted device includes:

a. a measurement function for acquiring the integrity metric of the computing apparatus;
b. an authentication function for authenticating a user's smart card; and
c. a controller for interacting with the main processing means and the measurement and authentication functions.

54. (New) Computing apparatus as claimed in claim 53 wherein said measurement function has access to memory in said trusted device for storing a private key of the trusted device and the integrity metric, the integrity metric indicating whether or not the trusted device was accessed by the main processor before said main processor accesses basic input/output instructions for booting the computing apparatus.